WEB APPLICATION FIREWALL

FortiWeb™ 5.1 Patch 2

NMI & COMlog Technical Note

Courtney Schwartz

Contributors:
Hao Xu
Yang Song

FortiWeb 5.1 Patch 2 NMI & COMlog Technical Note

February 14, 2014

1st Edition

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forum
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Introduction

FortiWeb hardware and FortiWeb-VM virtual appliance models are available that are suitable for medium and large enterprises, as well as service providers. Non-maskable interrupt (NMI) and COMlog are one of the features introduced specifically to support advanced debugging and troubleshooting that may be required by large service providers.

Supported platforms include:

- FortiWeb 3000C
- FortiWeb 3000CFsx
- FortiWeb 3000D
- FortiWeb 4000C
- FortiWeb 4000CFsx
- FortiWeb 4000D

COMlog

When errors occur, the kernel and many FortiWeb daemons output messages to the console. However, if you do not have a computer attached to FortiWeb's serial console port, or are not saving the output to a file while the errors are occurring, errors may scroll by too quickly for you to be able to read them. It will also be difficult to send them to Fortinet Technical Support. For tickets involving the kernel and daemon debugging, these error messages can be important.

To solve this, instead of keeping a computer attached to FortiWeb, you can save console output to a file on the FortiWeb appliance's internal flash disk by enabling COMlog, and then use the CLI to download the error messages later.

COMlog can record up to 500,000 daemon and/or kernel log messages. If the COMlog disk partition is full when a new COMlog message is generated, FortiWeb will rotate the log — that is, delete the oldest message in order to store the newest one.

To enable COMlog to store daemon or kernel errors, enter these CLI commands:

```
diagnose debug comlog daemon enable
diagnose debug comlog kernel enable
```

To display the enabled/disabled status of COMlog, the time range of its stored log messages, and the number of stored messages, enter these CLI commands:

```
diagnose debug comlog info status
diagnose debug comlog info time
diagnose debug comlog info logcount
```

When you have accumulated enough error messages and you want to download them to your computer, start your terminal emulator and prepare it to save CLI output to a file. Steps vary by terminal emulator. For example, in PuTTY, change your session logging settings to save printable output to a file such as `daemon-errors.txt`, then connect to the FortiWeb CLI. Then, to disable COMlog and to show the 1000 newest messages, enter these CLI commands:

```
diagnose debug comlog daemon show
diagnose debug comlog kernel show
```

To delete messages stored by COMlog, enter these CLI commands:

```
diagnose debug comlog daemon clear
diagnose debug comlog kernel clear
```

Non-maskable interrupt (NMI)

Some hardware models of FortiWeb have an NMI pinhole for the interrupt controller. In a special build of FortiWeb 4.0 MR4 Patch 7, and in FortiWeb 5.0 Patch 2 and later, there is firmware support for this — an NMI watchdog can be used to gather advanced kernel-level registers and call stack traces from all CPUs. Since many networking functions are performed by the kernel, NMI output can include some network debugging information also.

NMI is useful in rare cases such as when system hangs cannot be interrupted any other way, or if a kernel panic has occurred resulting in a halting state, and you want to gather forensic data to provide to Fortinet Technical Support for analysis in order to diagnose and fix the cause.

If you have enabled COMlog in the CLI, you do not need to connect to the console. You can use COMlog to store NMI output instead.

To gather NMI output via console

1. Connect a console or computer with a terminal emulator such as PuTTY or Tera Term to the serial port.
2. Configure your terminal to save CLI output to a text file. (In PuTTY, for example, configure session logging to save printable output to a text file.)
3. On your FortiWeb appliance, use a pin or needle to press the interrupt button. To find the NMI button on your model, see your model's newest *QuickStart Guide*.

   Your FortiWeb appliance will output a kernel dump to your serial CLI connection, then reboot.
4. Save the text file and close your CLI session. (In PuTTY, the file will be flushed to disk when you close the application.)
5. Send the kernel dump text file to Fortinet Technical Support.

Example output

```
2013-07-14 14:35:50 <4>NMI backtrace for cpu 0
2013-07-14 14:35:50 <4>CPU 0
2013-07-14 14:35:50 <4>Modules linked in: arpfilter bridge_mac
ti_bridge share_ip intf_filter bpctl_mod cp7vpn miglog admin_socket
2013-07-14 14:35:50 <4>
2013-07-14 14:35:50 <4>Pid: 0, comm: swapper Not tainted 2.6.38.8+ #2
Dell Inc. PowerEdge R710/0NC7T0
2013-07-14 14:35:50 <4>RIP: 0010:[<ffffffff8020892b>]
[<ffffffff8020892b>] mwait_idle+0x72/0x75
2013-07-14 14:35:50 <4>RSP: 0018:ffffffff80639f60  EFLAGS: 00000246
2013-07-14 14:35:50 <4>RAX: 0000000000000000 RBX: ffffffff80638010 RCX:
0000000000000000
2013-07-14 14:35:50 <4>RDX: 0000000000000000 RSI: ffffffff80639fd8 RDI:
ffffffff806fe108
2013-07-14 14:35:50 <4>RBP: ffffffff8068fd58 R08: 0000000000000000 R09:
ffff880325cf7da4
2013-07-14 14:35:50 <4>R10: 0000000000000000 R11: ffff880325cf7f18 R12:
6db6db6db6db6db7
2013-07-14 14:35:50 <4>R13: ffffffff806d4310 R14: ffffffff806d4e20 R15:
0000000000000000
2013-07-14 14:35:50 <4>FS:  0000000000000000(0000)
GS:ffff8800cf000000(0000) knlGS:0000000000000000
2013-07-14 14:35:50 <4>CS:  0010 DS: 0000 ES: 0000 CR0:
000000008005003b
2013-07-14 14:35:50 <4>CR2: 00007f327cb890a4 CR3: 0000000324fb6000 CR4:
00000000000006f0
2013-07-14 14:35:50 <4>DR0: 0000000000000000 DR1: 0000000000000000 DR2:
0000000000000000
2013-07-14 14:35:50 <4>DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7:
0000000000000400
2013-07-14 14:35:50 <4>Process swapper (pid: 0, threadinfo
ffffffff80638000, task ffffffff80661020)
2013-07-14 14:35:50 <0>Stack:
2013-07-14 14:35:50 <4> ffffffff802012f6 0000000000000000
0000000000000000 0000000000000000
2013-07-14 14:35:50 <4> ffffffff806a7c3f 0000000000000000
0000000000000000 ffffffff806d4e20
2013-07-14 14:35:50 <4> 0000000000090000 0000000000000000
0000000000000000 0000000000000000
2013-07-14 14:35:50 <0>Call Trace:
2013-07-14 14:35:50 <4> [<ffffffff802012f6>] ? cpu_idle+0x4d/0x7e
2013-07-14 14:35:50 <4> [<ffffffff806a7c3f>] ? start_kernel+0x331/0x33d
2013-07-14 14:35:50 <4> [<ffffffff806a7398>] ?
x86_64_start_kernel+0xf3/0xf9
2013-07-14 14:35:50 <0>Code: 8b 34 25 88 b5 00 00 31 c9 48 8d 86 38 e0
ff ff 48 89 ca 0f 01 c8 0f ae f0 48 8b 86 38 e0 ff ff a8 08 75 08 48 89
```

```
c8 fb 0f 01 c9 <c3> fb c3 fb 65 48 8b 04 25 88 b5 00 00 48 8d 90 38 e0
ff ff eb
2013-07-14 14:35:50 <4>Call Trace:
2013-07-14 14:35:50 <4> [<ffffffff802012f6>] ? cpu_idle+0x4d/0x7e
2013-07-14 14:35:50 <4> [<ffffffff806a7c3f>] ? start_kernel+0x331/0x33d
2013-07-14 14:35:50 <4> [<ffffffff806a7398>] ?
x86_64_start_kernel+0xf3/0xf9
2013-07-14 14:35:50 <4>Pid: 0, comm: swapper Not tainted 2.6.38.8+ #2
2013-07-14 14:35:50 <4>Call Trace:
2013-07-14 14:35:50 <4> <NMI>  [<ffffffff8020399f>] ?
do_nmi+0x196/0x1ef
2013-07-14 14:35:50 <4> [<ffffffff804df43a>] ? nmi+0x1a/0x20
2013-07-14 14:35:50 <4> [<ffffffff8020892b>] ? mwait_idle+0x72/0x75
2013-07-14 14:35:50 <4> <<EOE>>  [<ffffffff802012f6>] ?
cpu_idle+0x4d/0x7e
2013-07-14 14:35:50 <4> [<ffffffff806a7c3f>] ? start_kernel+0x331/0x33d
2013-07-14 14:35:50 <4> [<ffffffff806a7398>] ?
x86_64_start_kernel+0xf3/0xf9
2013-07-14 14:35:50 <6>sending NMI to all CPUs:
2013-07-14 14:35:50 <4>NMI backtrace for cpu 1
2013-07-14 14:35:50 <4>CPU 1
2013-07-14 14:35:50 <4>Modules linked in: arpfilter bridge_mac
ti_bridge share_ip intf_filter bpctl_mod cp7vpn miglog admin_socket
2013-07-14 14:35:50 <4>
2013-07-14 14:35:50 <4>Pid: 0, comm: kworker/0:0 Not tainted 2.6.38.8+
#2 Dell Inc. PowerEdge R710/0NC7T0
2013-07-14 14:35:50 <4>RIP: 0010:[<ffffffff8020892b>]
[<ffffffff8020892b>] mwait_idle+0x72/0x75
2013-07-14 14:35:50 <4>RSP: 0018:ffff88032fdcff30  EFLAGS: 00000246
2013-07-14 14:35:50 <4>RAX: 0000000000000000 RBX: ffff88032fdce010 RCX:
0000000000000000
2013-07-14 14:35:50 <4>RDX: 0000000000000000 RSI: ffff88032fdcffd8 RDI:
ffffffff806fe108
2013-07-14 14:35:50 <4>RBP: ffffffff8068fd58 R08: 0000000000000000 R09:
ffff880325c99da4
2013-07-14 14:35:50 <4>R10: 0000000000000000 R11: ffff880325c99f18 R12:
0000000000000000
2013-07-14 14:35:50 <4>R13: 0000000000000000 R14: 0000000000000000 R15:
0000000000000000
2013-07-14 14:35:50 <4>FS:  0000000000000000(0000)
GS:ffff8800cf020000(0000) knlGS:0000000000000000
2013-07-14 14:35:50 <4>CS:  0010 DS: 0000 ES: 0000 CR0:
000000008005003b
2013-07-14 14:35:50 <4>CR2: 00007f0414ae1000 CR3: 0000000325136000 CR4:
00000000000006e0
2013-07-14 14:35:50 <4>DR0: 0000000000000000 DR1: 0000000000000000 DR2:
0000000000000000
2013-07-14 14:35:50 <4>DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7:
0000000000000400
2013-07-14 14:35:50 <4>Process kworker/0:0 (pid: 0, threadinfo
ffff88032fdce000, task ffff88032fc53c80)
```

```
2013-07-14 14:35:50 <0>Stack:
2013-07-14 14:35:50 <4> ffffffff802012f6 0000000000000282
0000000000000000 0000000000000000
2013-07-14 14:35:50 <4> 0000000000000000 0000000000000000
0000000000000000 0000000000000000
2013-07-14 14:35:50 <4> 0000000000000000 0000000000000000
0000000000000000 0000000000000000
2013-07-14 14:35:50 <0>Call Trace:
2013-07-14 14:35:50 <4> [<ffffffff802012f6>] ? cpu_idle+0x4d/0x7e
2013-07-14 14:35:50 <0>Code: 8b 34 25 88 b5 00 00 31 c9 48 8d 86 38 e0
ff ff 48 89 ca 0f 01 c8 0f ae f0 48 8b 86 38 e0 ff ff a8 08 75 08 48 89
```

(Output abbreviated)

```
2013-07-14 14:38:49 <4>intf name : port8
2013-07-14 14:38:49 <4>protocol : 17
2013-07-14 14:38:49 <4>port : 162
2013-07-14 14:38:49 <4>action = 0
2013-07-14 14:38:49 <4>
2013-07-14 14:38:49 <4>------------------------------------------------
2013-07-14 14:38:49 <4>in device open
2013-07-14 14:38:49 <4>The deploy mode is = 4
2013-07-14 14:38:49 <4>-----------------bridge_ctrl:is_module_enable =
0-------------------
2013-07-14 14:38:49 <4>Invalid ioctl_cmd
2013-07-14 14:38:49 <4>in device open
2013-07-14 14:38:49 <4>Value of Syn cookie = 1,mode:4
2013-07-14 14:38:49 <4>in device open
2013-07-14 14:38:49 <4>max half open session = 2000
2013-07-14 14:38:49 <6>bnx2 0000:02:00.0: port3: NIC Copper Link is Up,
1000 Mbps full duplex, receive & transmit flow control ON
2013-07-14 14:38:49 <6>bnx2 0000:01:00.0: port1: NIC Copper Link is Up,
1000 Mbps full duplex
2013-07-14 14:38:49 <6>bnx2 0000:01:00.1: port2: NIC Copper Link is Up,
1000 Mbps full duplex
2013-07-14 14:38:49 <6>bnx2 0000:02:00.1: port4: NIC Copper Link is Up,
1000 Mbps full duplex, receive & transmit flow control ON
2013-07-14 14:38:49 <4>User space programme pid is :1395
2013-07-14 14:38:49 <6>warning: process `updated' used the deprecated
sysctl system call with 1.34.
```